ON SECURITY AND OPPORTUNISTIC ROUTING IN WIRELESS SENSOR NETWORKS

Synopsis submitted in fulfillment of the requirements for the Degree of

DOCTOR OF PHILOSOPHY

By

NAGESH KUMAR

Enrolment No. 136214

Under the Supervision of

Dr. Yashwant Singh and Dr. Pradeep Kumar Singh

Department of Computer Science Engineering and Information Technology

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY

Waknaghat, Solan-173234, Himachal Pradesh, INDIA

April, 2018

Table of Contents

Content	Page Number
Abstract	**iii**
CHAPTER 1 INTRODUCTION AND MOTIVATION	**1**
1.1 Introduction	**1**
1.2 Genesis of Problem	**1**
1.3 Problem Statement	**1**
1.4 Objectives	**1**
1.5 Approach Followed	**2**
1.6 Contributions	**2**
1.7 Chapter's Layout	**2**
CHAPTER 2 REVIEW OF LITERATURE	**3**
2.1 Introduction	**3**
2.2 Routing Categorization and Analysis	**3**
2.3 Related Work	**3**
2.3.1 Trust Aware Routing in WSN	**4**
2.3.2 Packet Load Balancing based OR Protocols	**4**
2.4 Parameters of Evaluation	**4**
CHAPTER 3 ENERGY EFFICIENT OPPORTUNISTIC ROUTING METRIC	**5**
3.1 Introduction	**5**
3.2 Proposed OR Metric: Energy Depletion Factor (EDF)	**5**
3.2.1 Energy Cost Model	**5**
3.2.2 Energy Depletion Factor	**5**
3.3. Experimental Results and Performance Analysis	**6**
3.3.1 Simulation Scenario	**6**
3.3.2 Results and Analysis	**6**
CHAPTER 4 ENERGY EFFICIENT OPPORTUNISTIC ROUTING PROTOCOL	**8**
4.1 Introduction	**8**
4.2 Proposed OR Protocol	**8**
4.2.1 Models and Assumptions	**8**
4.2.2 Proposed OR Protocol	**8**
4.3. Experimental Results and Performance Analysis	**9**
4.3.1 Simulation Scenario	**9**
4.3.2 Results and Analysis	**9**
CHAPTER 5 TRUST AWARE OPPORTUNISTIC ROUTING METRIC	**11**
5.1 Introduction	**11**
5.2 Proposed Trust Aware OR Metric	**11**

5.2.1 Phase 1: Identification of Elements 11
5.2.2 Phase 2: Trust Evaluation 12
5.3 Experimental Results and Performance Analysis 13
5.3.1 Simulation Setup 13
5.3.2 Experimental Results 13
CHAPTER 6 TRUST AWARE AND ENERGY EFFICIENT OPPORTUNISTIC ROUTING 15
6.1 Introduction 15
6.2 Modified_MDOR 15
6.2.1 Forwarder Selection Metric 15
6.2.2 Algorithm 16
6.2.3 Experimental Results and Performance Analysis 16
6.3 TAEROR: OR Protocol for WSN 17
6.3.1 Relay Selection Algorithm 18
6.3.2 Experimental Results and Performance Analysis 19
CHAPTER 7 TRUST AND LOAD BALANCING BASED OPPORTUNISTIC ROUTING PROTOCOL 20
7.1 Introduction 20
7.2 Proposed OR Protocol (TPBOR) 20
7.2.1 Relay Selection Criteria 20
7.2.2 Trust and Packet load Balancing Based OR (TPBOR) 21
7.3 Experimental Results and Performance Analysis 21
7.3.1 Results and Discussions 21
CHAPTER 8 CONCLUSION AND FUTURE SCOPE OF WORK 23
8.1 Introduction 23
8.2 Comparative Analysis 23
8.3 Future Perspectives 23
References 24
List of Publications 26

ABSTRACT

The sensor networks are the result of advancements in micro-technologies and are increasing in demand. In wireless sensor networks (WSN), the data must reach to an infrastructure processing node. The sensor nodes follow a common communication pattern by using routing mechanisms. Routing is the most important phase of network operations because the sensor nodes have limited resources to perform all the network operations. Traditional routing protocols cannot cope up with the failures and malicious activities in unstable application environments. Therefore alternative methods must be designed and researched to achieve performance goals.

The opportunistic routing (OR) in wireless sensor networks (WSN) is gaining popularity due to high throughput, low delays, and good packet delivery ratios. Providing data integrity, availability and reliability with less energy exhaustion are very important in WSN. To achieve all of these properties, the routing protocols must ensure the security of route selection process to avoid the participation of malicious nodes. Also, there is a need for energy conservation while providing security to increase the network lifetime and throughput. This thesis work is carried out to optimize energy efficiency, security of route selection process and equal distribution of packet load among all nodes in the network. Firstly, to provide energy efficiency OR metric named as energy depletion factor (EDF) is proposed which distributes the energy consumption load among all nodes equally in the network. The metric calculates the impact of each transmission and reception on the residual energy of each node. Secondly, an energy efficient OR protocol is proposed by using EDF, which improves energy efficiency, delays, and throughput of the network.

To provide the security for route selection process, trust management OR metric is proposed. Based on this metric a new trust-aware and energy efficient opportunistic routing protocol (TAEROR) is proposed which avoids malicious nodes to be a part of the routing process. This protocol increases throughput and lifetime of the network. To reduce the congestion in the network the thesis presents a new trust and packet load balancing OR protocol (TPBOR). This protocol involves queue size of each sensor node in relay selection process. This will reduce the congestion inside a single relay node and distribute the packet load among all relay nodes. This thesis balances between energy, security and traffic load inside the network. The proposed work may be utilized in different applications of WSN where; energy, network lifetime and throughput are important factors.

CHAPTER 1
INTRODUCTION AND MOTIVATION

1.1 Introduction

Wireless sensor networks (WSN) are increasing in demand due to the abilities of sensor nodes to be deployed in unattended environments [1] [2]. The sensor nodes are able to collect data via sensors and are able to communicate the same through small radio, toward the end-users. Opportunistic routing (OR) for WSN is an energy efficient communication technique which involves almost every sensor node of the network to participate in the communication process. This technique utilizes the broadcasting nature of wireless networks [4].

1.2 Genesis of Problem

Networking the sensor nodes which are left unattended in outside environment will affect the application like forest fire detection, target tracking, and other disaster management applications. Fixed path routing techniques will suffer a lot in the presence of malicious nodes [5]. Opportunistic routing (OR) may overcome the problems in fixed path routing by utilizing the broadcasting nature of wireless radios. Due to broadcasting nature OR protocols may be exposed to internal or external attacks. The major research gaps in existing opportunistic routing protocols are: lack of energy efficiency, security of routing process and balancing the transmission load among all relay nodes.

1.3 Problem Statement

In the development of opportunistic routing protocols for WSN, there is a need for answering certain questions: Can routing processes able to distribute the load of energy consumption equally among all the nodes? If yes, then how can this be made possible as OR is broadcasting in nature? If the energy efficiency is achieved through equal distribution, how to tackle the problem of high end-to-end delays? Can routing approach reduce the duplicate packets by using a coordination mechanism for relay nodes? How opportunistic routing will detect and avoid malicious nodes with optimum utilization of resources? How the packet transmission load will be distributed among all nodes equally?

1.4 Objectives

The following objective has been formulated, on the basis of the above problem statement and achieved in this research work.

a) To develop a new energy efficient opportunistic routing metric, which will distribute the energy consumption load equally among all nodes in the network.
b) To develop a new energy efficient opportunistic routing protocol for WSN, which will improve the throughput of the network and also reduce the end-to-end delay.
c) To develop a trust and reputation based OR metric, which will avoid the malicious and selfish nodes during the routing process.
d) To develop a secure and energy efficient OR protocol, which will improve the network lifetime and avoid the malicious nodes during the routing process.
e) To optimize between security, energy, and packet load in WSN.

1.5 Approach Followed

The research gaps were identified on the basis of literature. After research gaps, certain parameters are identified which can be used to improve the performance of the network. To improve the energy efficiency of the network, there must be the distribution of energy load among all the nodes. To achieve this task the most important factor are combined to form a composite routing metric. For improving the network performance further in terms of end-to-end delays and throughput, a new opportunistic routing metric was proposed. The approach used to propose a new OR protocol was to identify the factors which can cause the various performance issues. Next, to fulfill the gap of security breach inside the network, the main security holes were identified. Out of these holes, the important ones were identified and a composite metric was proposed. To handle the problems with the proposed trust-aware routing metric, a trust-aware OR protocol is devised. Firstly the trust-aware routing protocol was defined by taking existing MDOR [7] protocol as base protocol. After testing this protocol on NS2 it is being observed that the trust-aware protocols may improve the performance of the network. Based on this assumption a new protocol was proposed which improve the performance of the network. To overcome the problem of overloaded nodes a new approach was proposed. To tackle with packet load a new load balancing factor was proposed, which involve the buffer size of each relay node. The current buffer size was tested for each node selected as a next-hop forwarder.

1.6 Contributions

The thesis will explore the various routing mechanisms proposed for WSN to improve the energy efficiency, security, and reliability. After the analysis of all communication protocols and their categories, it is being observed that opportunistic routing protocols may present better results than other fixed path routing protocols. An opportunistic routing metric name as energy depletion factor (EDF) proposed in chapter 3 to provide the energy efficiency for the network which was the first research gap. Another contribution presented in chapter 4 for improving these parameters further is the new opportunistic routing protocol which is energy efficient. Chapter 5 introduce a trust and reputation aware routing metric which is able to tackle this problem. To handle the problem of delays Chapter 6 provides two opportunistic routing protocols: modified_OR and TAEROR. Chapter 7 extends the work of Chapter 6 to include the buffer inspection of each relay node to develop new protocol TPBOR.

1.7 Chapter's Layout

Chapter 1 provides the basic introduction to thesis which contains WSN, problem statement and objectives mainly. **Chapter 2** discusses a detailed literature survey on WSN and communication protocols for the same. **Chapter 3** will discuss the newly proposed energy efficient OR metric named as energy depletion factor (EDF). EDF is used to develop a new OR protocol presented in **Chapter 4. Chapter 5** will present a solution to tackle the problem of malicious nodes and selfish nodes. **Chapter 6** provides a detailed discussion of two newly proposed trust-aware and reliable OR protocols. **Chapter 7** discuss the solution to load balancing problem during routing process in WSN. **Chapter 8** gives the conclusions after comparing the three proposed trust-aware protocols and an evaluation of the contributions in the thesis is presented. This chapter also describes direction for the future work.

CHAPTER 2
REVIEW OF LITERATURE

2.1 Introduction

WSN contains sensor nodes with wireless radios, which are able to communicate on short ranges. The pictorial representation can be seen in figure 2.1, which represent both wireless sensor networks and the major components of a sensor node. The nodes in WSN are densely scattered and networking these nodes is a tough task as it affects the performance of network. The protocols are required to use these resources efficiently so that the network can be used for longer times.

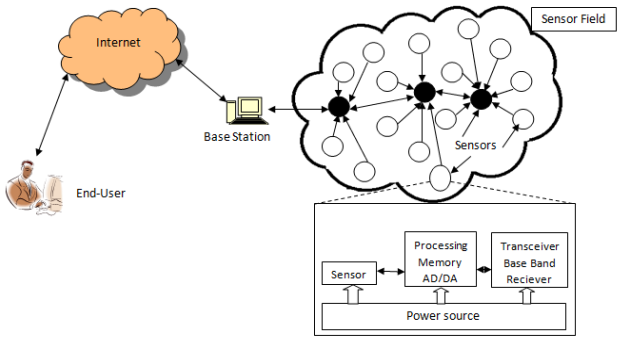


Figure 2.1 WSN Communication Architecture Including Sensor Node Components

2.2 Routing Categorization and Analysis

The routing protocols proposed by different authors over the years have been classified by many authors [1] [3]. Mostly the routing protocol for WSN can be differentiated on the basis of their working and data collection abilities.

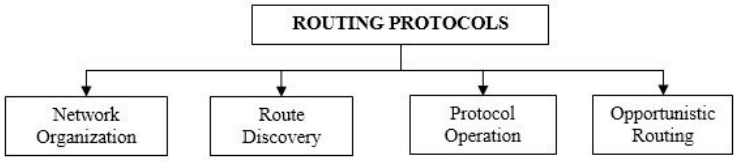


Figure 2.2 Categorization of Routing Protocols

2.3 Related Work

Opportunistic routing (OR) for WSN is an energy efficient communication technique which involve almost every sensor node of the network to participate in communication process. The protocols studied are as discussed below. Ex-OR is first protocol proposed by [4] in the category of opportunistic routing. Here, MAC and routing mechanisms were collaborated to make the final decision of route selection. EEOR is another protocol proposed in [9] was an energy efficient OR protocol. There were two cases discussed in this protocol for constant transmission power and dynamic transmission power. This protocol was simulated and tested for performance on TOSSIM simulator EFFORT is also an energy efficient OR protocol proposed by [8] maximize the lifetime of wireless sensor network. Authors have proposed a routing metric which is opportunistic in nature. The metric is based on the residual energy of

the node and calculated globally from source to destination always. EOMR proposed in [10] is purely meant to reduce the energy cost for wireless sensor network. Rather than using broadcasting this protocol use multicast mechanism to transmit data packets toward the base station. MDOR is proposed in [7] considers that choosing a node which is far away from source node but nearer to destination and vice versa cannot be a solution to solve the energy consumption problem. QEOR was proposed in [11] is a protocol proposed recently to provide QoS with lesser energy consumption for WSN. The authors have proposed that QoS and energy efficiency are critical to be achieved together.

2.3.1 Trust Aware Routing in WSN

Whenever it comes to security of the network cryptographic systems will come to the mind of every researcher. For security, trust management systems can be used. Some of the trust aware protocols used in thesis for comparison are discussed below. In [12] authors have proposed a trust and location aware routing (TLAR) protocol for WSN. The objective of TLAR was to provide a lightweight and dependable routing algorithm for WSN. In [13] proposed a new trust aware routing protocol named as trust and energy aware secure routing protocol (TESRP) for sensor and actuator networks. Another efficient routing protocol for WSN is trust aware opportunistic Routing (TAOR) [14]. This protocol was energy efficient and also reduces the end-to-end delays. Trust management systems can build up coordination among nodes and avoid malicious nodes in routing process.

2.3.2 Packet Load Balancing based OR Protocols

Load balancing of packet transmission is required when there is a continuous data flow in the network. The buffers of relay nodes gets full and the incoming packets are either dropped or face high delays [6]. In [15] authors have proposed a buffer aware opportunistic routing (BAOR) mechanism which combine the location and buffer length of relay nodes to assign priorities. In [16] authors have proposed a packet based opportunistic routing protocol (POR) which has used packet-piggyback-overhearing technique to schedule the packet delivery by different source nodes.

2.4 Parameters of Evaluation

The proposed protocols are compared with existing protocols by using these parameters. These parameters are commonly used for comparative analysis of routing protocols. If these parameters are optimal than the network will give good output and reliable results. The parameters are: 1) Energy Consumption, 2) Network Lifetime, 3) End-to-End Delay, 4) Path Loss, 5) Packet Delivery Ratio (PDR), 6) Throughput and 7) Risk Level

CHAPTER 3
ENERGY EFFICIENT OPPORTUNISTIC ROUTING METRIC

3.1 Introduction

This chapter presents a new energy-aware OR metric for WSN called as an energy depletion factor (EDF). EDF is designed on the basis of residual energy of a node. It considers energy consumed during transmission, retransmission, and reception of data packets and acknowledgments during the network operation. EDF can be used directly with existing OR protocols for WSN. Expected transmission count (ETX) [4] was the first proposed as an OR metric for wireless networks. This metric selected the optimal path on the basis of the lesser number of hop counts.

3.2 Proposed OR Metric: Energy Depletion Factor (EDF)

EDF takes into account the residual energy of a node and calculates the impact of each transmission and reception of data packets. The basic energy consumption and EDF model will be discussed in following subsections.

3.2.1 Energy Cost Model

A sensor will consume E_{Trans} energy when it transmits an n-bit data packet over distance l, it will be given by the equation (1) below:

$$E_{Trans}(n,l) = \begin{cases} n.E_{R_elect} + n.E_{R_fs}.l^2, & if\ l < l_0 \\ n.E_{R_elect} + n.E_{R_amp}.l^4, & if\ l \geq l_0 \end{cases} \quad \text{..... (1)}$$

E_{R_elect} is the electronic energy consumed by a radio of a node to receive or transmit a data packet. When a sensor node receives n bit packet, it will ingest $E_{Recieve}$ amount energy given by equation (2) below:

$$E_{\text{Re}ceive}(n) = n.E_{R_elect} \quad \text{..... (2)}$$

Whenever a forwarder candidate node has to send an n-bit data packet to the base station, its radio circuit consumes, $E_{Forward}$ energy calculated by equation (3).

$$\begin{aligned} E_{Forward}(n,l) &= E_{Trans}(n,l) + E_{\text{Re}ceive}(n) \\ &= \begin{cases} 2n.E_{R_elect} + n.E_{R_fs}.l^2, & if\ l < l_0 \\ 2n.E_{R_elect} + n.E_{R_amp}.l^4, & if\ l \geq l_0 \end{cases} \end{aligned} \quad \text{..... (3)}$$

E_{R_amp} is the electronic energy consumed to amplify a data packet, where the distance is l.

3.2.2 Energy Depletion Factor

The proposed metric is named as EDF because it tells the routing protocol to resolve the next hop on the basis of residual energy. The metric calculates the impact of each transmission and reception on the residual energy of each node. The impact (SEC_{Ni}) on the residual energy (RE_{Ni}) of a node (Ni) by using energy consumption inside the node (EC) as follows from an equation (4).

$$SEC_{N_i} = \frac{EC}{RE_{N_i}} \quad \text{..... (4)}$$

a. **Transmission Impact ($E_{tx:Ni->fwd}$)**: $E_{tx:Ni->fwd} = \frac{E_{Trans}}{RE_{Ni}}$ ..... (5)

b. **Receiving Impact ($E_{rx:Ni}$)**: $E_{rx:Ni} = \frac{E_{Receive}}{RE_{Ni}}$ ..... (6)

c. **Retransmission Impact ($E_{re_tx:Ni->fwd}$)**: $E_{re_tx:Ni->fwd} = \frac{E_{Forward}}{RE_{Ni}}$ ..... (7)

d. **Acknowledgement Impact ($E_{ACK:Ni->source}$)**: $E_{ACK:Ni->source} = \frac{E_{Trans}}{RE_{Ni}}$ ..... (8)

All of these values will be aggregated to compute the overall impact, in form of EDF, of transmission and reception on the node's residual energy. EDF will be calculated at each relay node and this process will end only after the destination is reached as follows.

$$EDF_{Ni} = \frac{E_{tx:Ni->fwd} + E_{rx:Ni} + E_{re_tx:Ni->fwd} + E_{ACK:Ni->source}}{RE_{Ni}} \quad \text{..... (9)}$$

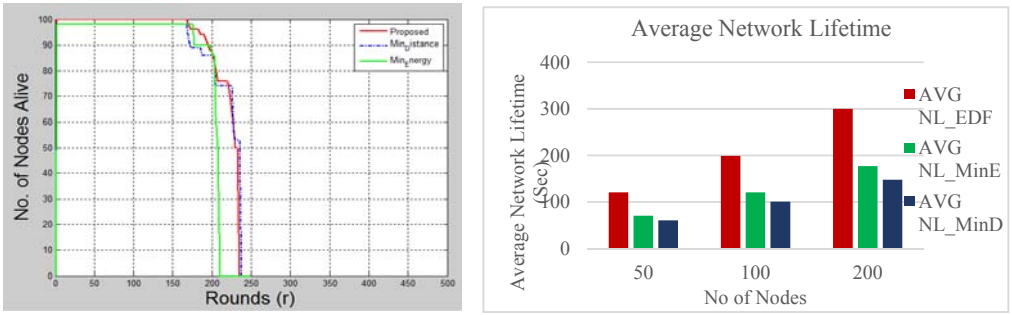
3.3 Experimental Results and Performance Analysis

3.3.1 Simulation Scenario

The nodes are randomly deployed in 500 x 500 m^2 area. Immediately, after complete deployment, nodes broadcast hello packets to collect the information about the neighbors. The protocols compared are: AODV_Min_Energy, AODV_Min_Distance, Proposed (AODV_EDF).

3.3.2 Results and Analysis

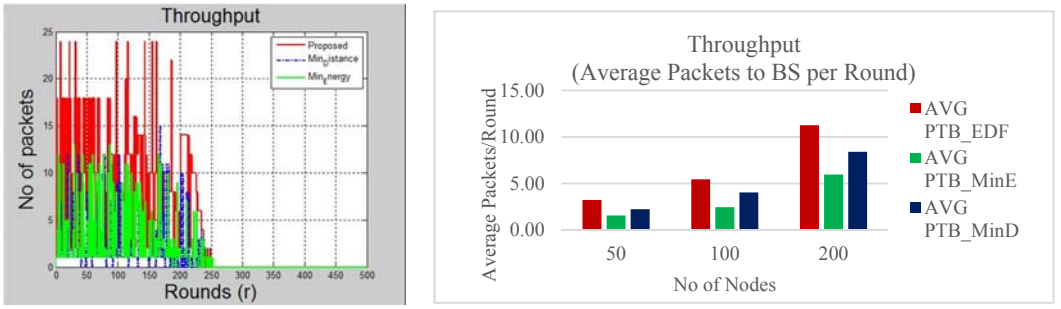
Network Lifetime: It is delineated as the total time elapsed from the starting time of the network and time at which the first networked sensor runs out of energy to transmit a data packet. Because to lose a node could mean that the network could lose some functionalities.



(a) **(b)**

Figure 3.1 a) Number of nodes alive after each round b) Average network lifetime in seconds

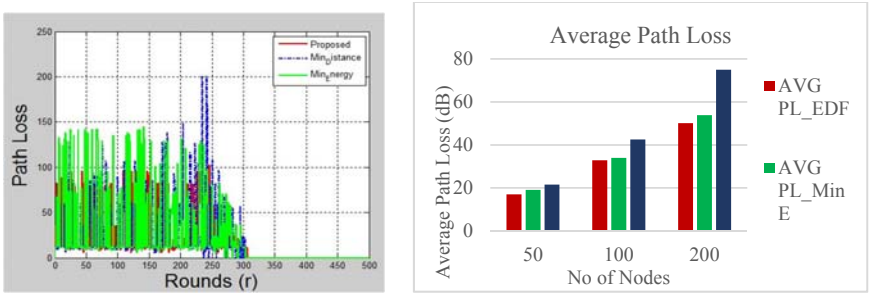
Throughput: Generally throughput is defined as the average number of packets transmitted from source to destination. Here in MATLAB, the simulation was performed in rounds and hence, the throughput is defined as an average number of packets transmitted towards the base station.



(a) **(b)**

Figure 3.2 a) Number of packets delivered at base station after each round b) Throughput

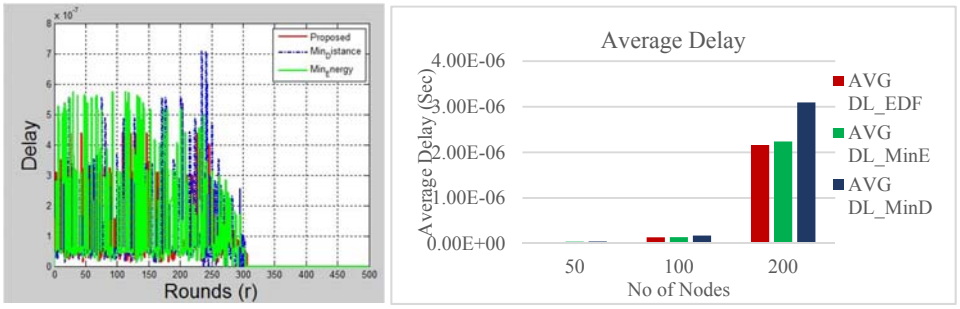
Path Loss: Free space path loss model has been considered for simulation purpose.



(a) **(b)**

Figure 3.3 a) Path loss calculated after each round b) Average Path Loss

End-to-end delay: This can be measured as the total time elapsed in transmitting a data packet from the source node and receiving the same at the base station.



(a) **(b)**

Figure 3.4 a) Delay calculated after each round b) Average end-to-end delay

CHAPTER 4
ENERGY EFFICIENT OPPORTUNISTIC ROUTING PROTOCOL

4.1 Introduction

Opportunistic routing (OR) for WSN is an energy efficient communication technique which involves almost every sensor node of the network to participate in the communication process. In this chapter, a new energy efficient opportunistic protocol has been proposed, simulated and evaluated on the basis of the simulation results.

4.2 Proposed OR Protocol

OR protocols discussed in related work considers energy efficiency as the main parameter in routing process and also all of these are based on opportunistic routing. This chapter also tries to introduce a new energy efficient opportunistic routing protocol for WSN. Before discussing the proposed protocol models and assumptions are presented as in the following subsection.

4.2.1 Models and Assumptions

This section gives an overview of the models and assumptions considered during simulation of the proposed approach. A wireless sensor network of N nodes deployed randomly over an area of size M x M is considered. This network can be seen like a graph. Energy consumption model is same as in chapter 2.

4.2.2 Proposed OR Protocol

This section will briefly discuss the proposed OR protocol. In start phase is the initializing phase of proposed OR protocol. This phase begins immediately after the deployment of sensor nodes in the field. Also, this phase will be repeated periodically. The nodes contact each other via sending hello messages.

Node_ID	Location	REP_Count	Energy

Figure 4.1 Neighbor Table Elements

From the neighbor table, the eligible forwarder candidate nodes have to be selected. To construct a forwarder set *PRR* has been calculated using following equation:

$$PRR_i = \frac{REP_Count_i}{PG_{source}} \quad \ldots\ldots\ldots\ldots\ldots (4)$$

where REP_Count_i is the reply count for a neighbor i and PG_{source} is the total number of hello packets generated at the source node. Each node which is having *PRR* greater than the threshold (0.2) has been added to forwarder list of the node i. This process is repeated for each new data transmission process. The forwarder list elements can be seen in Figure 4.2. The forwarder list has been sorted and a priority has been assigned to each forwarder.

Node_ID	Location	PDR	Priority

Figure 4.2 Forwarder Set Elements

After getting the forwarder set the network setup has been completed. Now the forwarder node has been selected on the go. EDF calculates the impact on the energy of a node during each reception and transmission. EDF of a node can be calculated as follows.

$$EDF_{Ni} = \frac{E_{tx:Ni->fwd} + E_{rx:Ni} + E_{re_tx:Ni->fwd} + E_{ACK:Ni->source}}{RE_{Ni}} \quad \ldots\ldots\ldots\ldots (6)$$

The description of each term is given in chapter 3. After calculation of EDF, if it is less than the threshold value (*EDF_th*) a timer has been set in the node with respect to the value of EDF.

Algorithm
Forwarder_Node_Selection (S=Source, D=Destination)
//When any node S want to send a packet towards D and it has already constructed a forwarder list, it will follow this algorithm
Begin
For each node, *i* Ɛ *FL (S)* repeat
    Calculate *EDF (i)*
    IF *EDF (i)* >= *EDF_th (node)*
        Set Timer (*i*):= value of EDF
    Else
        Remove node *i* from *FL (S)*
    endIF
endFor
IF Timer (*i*): = NULL
    Broadcast data packet as {*i*, *D*, *Coordinates (i)*, Data} from *i*
Else
    Wait for the timer to be Null
endIF
end

4.3 Experimental Results and Performance Analysis

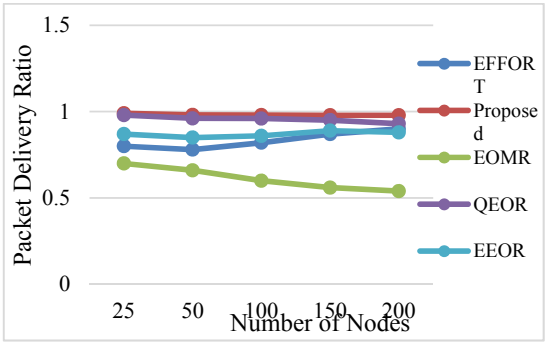
The working and results of the proposed algorithm are compared to existing energy aware opportunistic routing protocols EOMR [10], EEOR [9], EFFORT [8], and QEOR [11]. These all protocols are claimed to be energy efficient by the respective authors.

4.3.1 Simulation Scenario

All Compared protocols are simulated again using the network settings similar to the proposed protocol using NS2. After simulation, the results have been collected and plotted for better understanding.

4.3.2 Results and Analysis

Results are recorded and verified by performing extensive simulations for all analyzed protocols, including proposed protocol. Figure 4.3 presents the average packet delivery ratio for all compared protocols. The transmission delays are presented in form of average end-to-end delays introduced during the transmission and reception of data packets.



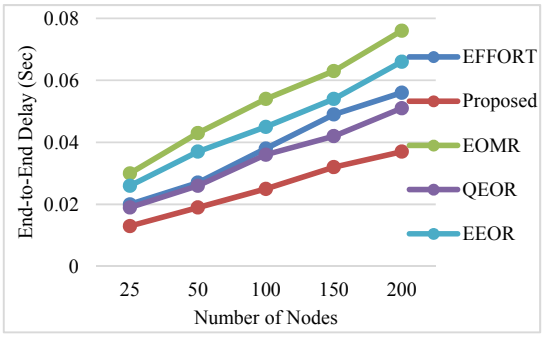
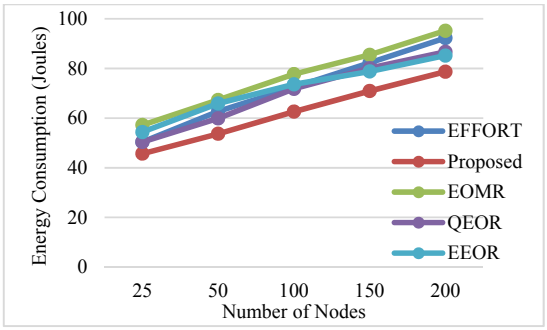


Figure 4.3 Packet Delivery Ratio

Figure 4.4 End-to-End Delay

Energy consumption is the main criteria for measuring the performance of energy efficient protocols for WSN.



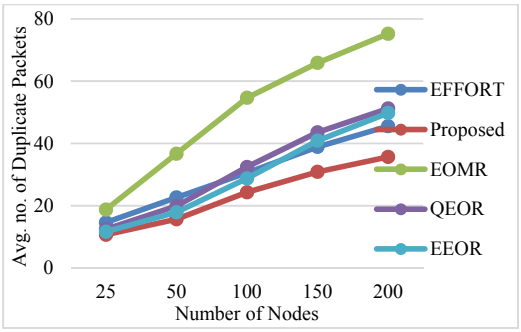


Figure 4.5 Energy Consumption

Figure 4.6 Average Duplicate Packets

Next analysis is the number of duplicate packets received at the base station. It can be seen from the figure 4.6 that the number of duplicate packets at the base station for the proposed protocol is lesser than other protocols. The network lifetime for proposed protocol increases considerably because of the improved energy efficiency.

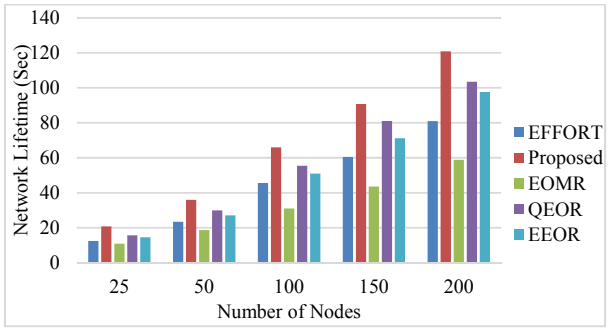


Figure 4.7 Average Network Lifetime based Comparison

Overall, by analyzing these all performance parameters, the proposed protocol shows improvement over the existing protocols. Proposed protocol balances the energy consumption in the network among all nodes and tries to keep each node alive for a long time. This will improve the network lifetime and throughput of the network.

CHAPTER 5
TRUST AWARE OPPORTUNISTIC ROUTING METRIC

5.1 Introduction

This chapter will present a new energy consumption and trust-aware OR metric which can work with any routing algorithm for WSN. The metric may be used with existing OR protocols for WSN to prolong network lifetime and increase the security of the routing process. The major contributions of this chapter are the newly proposed trust-aware metric and comparative analysis of the proposed metric by employing it to commonly used AODV [2] routing protocol.

5.2 Proposed Trust-Aware OR Metric

The data required by the metric are the ID of a node, residual energy and packet reception ratio (PRR). Each node will collect these values from neighbor nodes and calculates the packet forwarding ratio, acknowledgment sending and receiving ratio and residual energy based on energy consumption of a node. All of these parameters are then combined to form a composite routing metric. The in-between distance (D) of two sensor nodes is used to justify the progress of data packets (PFP) (eq 1 and eq 2). PFP specifies that the packet is making a positive progress towards the destination.

$$Dist_{i,j} = \sqrt{(x_co_i - x_co_j)^2 + (y_co_i - y_co_j)^2} \qquad \text{where } 0 \le i, j \le k \text{, and } i \ne j \tag{1}$$

$$PFP_{n_i}^{s,d} = Dist_{s,d} - Dist_{n_i,d} \qquad \text{where } s\text{=source, } d\text{=destination, } 0 \le n_i \le k \tag{2}$$

5.2.1 Phase 1: Identification of Elements

This is a data collection phase and packet reception ratio (*PRR*) is calculated for selecting only potential nodes for data transmission (eq 3).

$$PRR_i = \frac{P_{recieved}}{P_{sent}} \qquad \text{where } 0 \le PRR_i \le 1 \tag{3}$$

On the basis of *PRR* of a node *i* the potential forwarders are extracted from the neighbor list. The trust value for each node in the forwarder list has been calculated using following elements.

Sensor Node Identification (*ID*): This is the identity of a node which provides the values of location and remaining energy inside a node.

$$ID_i =< NodeID_i, Location_coordinates_i, Energy_i > \qquad \text{where } 0 \le i \le k$$

Forwarding Sincerity (*F*): This parameter depends on the value of successful and unsuccessful packet forwarding by a node in the forwarder list.

- F_i: Packet forwarding sincerity of node *i*
- FS_i: Packet forwarding success count of node *i*
- FF_i : Packet forwarding failure count of node *i*.

Energy Consumption (E_{total}): The energy consumed by a node to perform various network operations will be calculated by this element.

- E_{total_i} : Total residual energy of node *i*

$$E_{total} = E_{total} - (E_{tx} + E_{rx} + E_{ack}) \quad (4)$$

Where, E_{tx} : energy spent in transmitting a data packet, E_{rx} : energy spent in receiving a data packet, E_{ack} : energy spent in transmitting and receiving acknowledgments in the network.

Acknowledgement Sincerity (*ACK*): This element monitors the acknowledgments in the network.

- ACK_i : Acknowledgement sincerity of node *i*
- $SACK_i$: Successful acknowledgment count of node *i*
- $FACK_i$: Unsuccessful acknowledgment count of node *i*.

5.2.2 Phase 2: Trust Evaluation

In this phase, all the trust factors are evaluated. The values of trust factors are calculated and logged into the trust matrix.

Forwarding Sincerity (F_i)

$$F_i = \frac{FS_i - FF_i}{FS_i + FF_i}, \text{ subject to } 0 \le F_i \le 1 \quad (5)$$

Energy Depletion Value (E_{total_i})

$$E_{total_i} = \frac{E_{tx} + E_{rx} + E_{ack}}{E_{total}}, \text{ subject to } 0 \le E_{total_i} \le 1 \quad (6)$$

Acknowledgement Sincerity (ACK_i)

$$ACK_i = \frac{SACK_i - FACK_i}{SACK_i + FACK_i}, \text{ subject to } 0 \le ACK_i \le 1 \quad (7)$$

This will quantize the values of trust parameters. For each trust parameter, the weights are assigned according to their importance. The weight value for least important factors will be lower than that of important factors. Hence, all factor are combined to form a composite routing metric (T_i).

$$T_i = \frac{\alpha * F_i + \beta * E_{total_i} + \gamma * ACK_i}{\alpha + \beta + \gamma}, \text{ where } 0 \le \alpha, \beta, \gamma \le 1 \quad (8)$$

Here, $\frac{\alpha}{\alpha+\beta+\gamma}$ is the coefficient of forwarding sincerity factor (F_i), $\frac{\beta}{\alpha+\beta+\gamma}$ is the coefficient for energy consumption (E_{total_i}) and $\frac{\gamma}{\alpha+\beta+\gamma}$ is for acknowledgment sincerity factor (ACK_i). The trust value will be from 0 to 1 which means that the nodes having value 0 are malicious and untrusted.

5.3 Experimental Results and Performance Analysis

Here, DSDV has been chosen to apply the proposed metric. The modified DSDV will select next hop relay nodes on the basis of the proposed trust-aware OR metric. The modified DSDV will be compared to original DSDV [2] and AODV [2]. All of the protocols are simulated in MATLAB and applied for routing the packets in wireless sensor networks.

5.3.1 Simulation Setup

Simulation in MATLAB assumes 500 m X 500 m area for deployment of sensor nodes. Successful communication of data packets is considered only when the base station receives data packet accurately. A number of simulations were conducted in with one base station only. Continuous data communication has been considered for random deployment of N sensor nodes in the network.

5.3.2 Experimental Results

Safety Performance: Figure 5.1 below conclude that the proposed protocol employ security during routing process and can avoid malicious nodes easily as compared to normal AODV and DSDV.

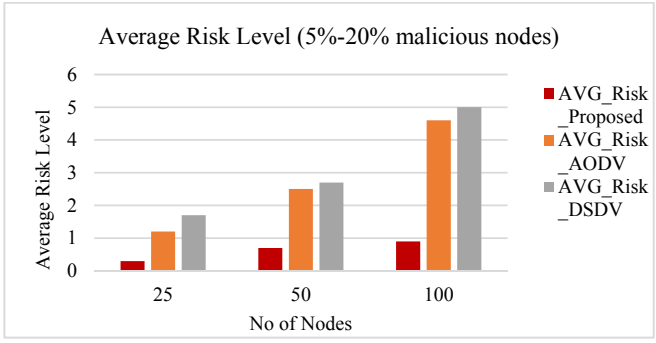


Figure 5.1 Average Risk Level

Energy Efficiency Performance: First order energy model [88] has been considered for measuring the performance of all of the compared protocols. Figure 5.2 depicts that an increase in a number of malicious nodes will also increase the energy consumption inside the network. This will reduce the network lifetime, but if the number of nodes is large in the network than the network lifetime will be increasing (figure 5.3).

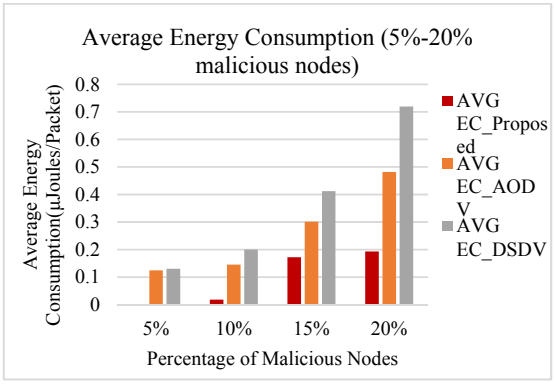


Figure 5.2 Average Energy Consumption

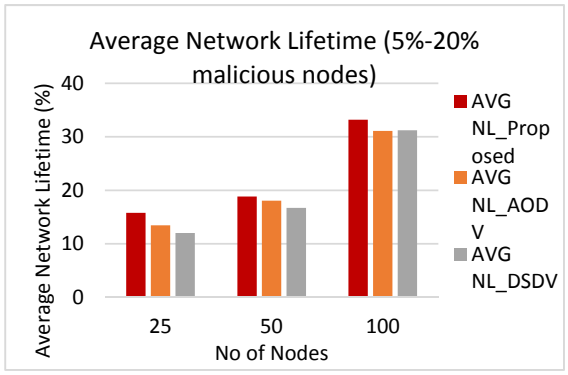


Figure 5.3 Average Network Lifetime

End-to-end delay (figure 5.4) will be increasing for the proposed protocol because of the calculation of routing metric and finding the best possible relay node according to trust value. In figure 5.5 the performance in terms of path loss in the presence of malicious nodes may be predicted.

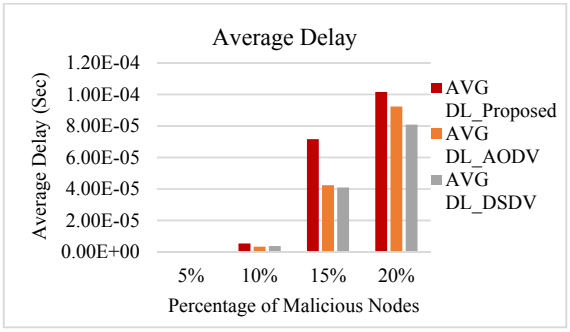


Figure 5.4 Average End-to-End Delay

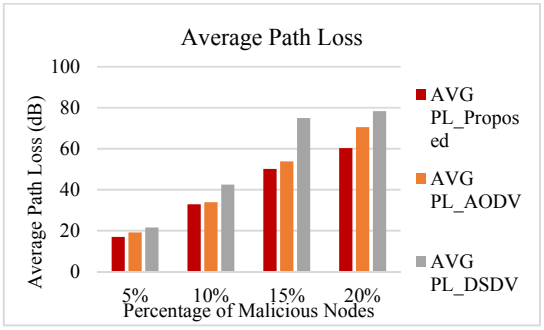


Figure 5.5 Average Path Loss

CHAPTER 6

TRUST AWARE AND ENERGY EFFICIENT OPPORTUNISTIC ROUTING

6.1 Introduction

This chapter proposes a new reputation-based OR metric and protocol. This metric considers energy efficiency and reputation of a node on the basis of packet forwarding ratio (PFR), to select next-hop candidate forwarders. The chapter proposes an extension to the previous work i.e. middle position dynamic energy OR algorithm. It is being extended to improve energy efficiency and provide reputation-based security to network and data.

6.2 Modified_MDOR

Middle position dynamic energy opportunistic routing (MDOR) [7] consider that each node has same capabilities but the transmission and reception energies of a radio may be different. The proposed protocol modified_MDOR considers trust value of each node to select the next-hop forwarder sensor node. This proposed protocol calculates the reputation of each neighbor node which are middle nodes considered in forwarder list.

6.2.1 Forwarder Selection Metric

This metric has two fragments: packet forwarding ratio and energy impact. The first fragment i.e. packet forwarding ratio (*PFR*) calculated as below

$$PFR_i = \frac{P_fwd_{i->next_hop}}{P_sent_{source->i}} \quad \text{..... (1)}$$

Where, $P_fwd_{i->next_hop}$ is the number of packets relayed by the node *i* towards its next-hop node and $P_sent_{source->i}$ is the number of packets sent by the source node towards node *i*.

Energy impact is the second part of the trust value which is based on the node's residual energy.

$$E_effect = \frac{E_{recieving} + E_{transmitting} + E_{ack_sending}}{E_{total}} \quad \text{..... (2)}$$

The receiving ($E_{recieving}$), transmitting ($E_{transmitting}$) and acknowledgment ($E_{ack_sending}$) energy consumptions are calculated by using the first order energy model given in MDOR [24]. Total energy (E_{total}) is the residual energy of a sensor node. These two parts i.e. *PFR* and E_{total} are combined to form a composite metric i.e. trust metric (*T_Value*) calculated by the following equation.

$$T_Value = \frac{\alpha.PFR + \beta.E_effect}{\alpha + \beta} \quad \text{..... (3)}$$

Here, α and β are the important factors for both trust value parts i.e. *PFR* and *E_effect* respectively. After the trust value is computed for every fellow node, the source node will run the modified_MDOR algorithm to find out the next-hop relay nodes.

6.2.2 Algorithm

Modified_MDOR starts functioning when any source node is having data to be sent to the base station. The node at the middle position of the neighbor list will be given higher priority to send data first. But, first trust value will be calculated for this higher priority node. If the trust value (*T_value*) is below a certain threshold then the node will be discarded from the neighbor list and marked as a malicious node.

Algorithm: Modified_MDOR (S, D)
Input: Source node S, Target node D, Distance(S, D).
Output: Successful transmission of a data packet from node S to node D

1. Define S as Source Node
2. Create neighbor list NGH for S
3. Sort neighbor list according to distance
4. if D is neighbor of S
5. Send data packets to D
6. else
7. FNL is the subset of NGH (FNL is the forwarder node list)
8. Select the middle node (FWD) from FNL i.e. (neither near to S nor near to T).
9. Calculate trust value (*T_Value*) for each middle node using equation 3.
10. if *T_Value* >= 0.2
11. Start communication with FWD
12. else
13. {
13. Discard FWD from FNL.
14. Select a second middle node from FNL and name it as FWD.
15. Repeat from step 9 to 14
16. }
17. if FWD is equal to D then stop the algorithm
18. else repeat step 2 to step 18 until D is reached

6.2.3 Experimental Results and Performance Analysis

To test the performance of proposed protocol simulations have been performed. Results are compared to base protocol MDOR [7] and trust-aware recently proposed routing protocol i.e. TLAR [12]. The performance of modified_MDOR, MDOR and TLAR are recorded and plotted in form of graphs. The performance parameters are packet delivery ratio, energy consumption and end-to-end delay.

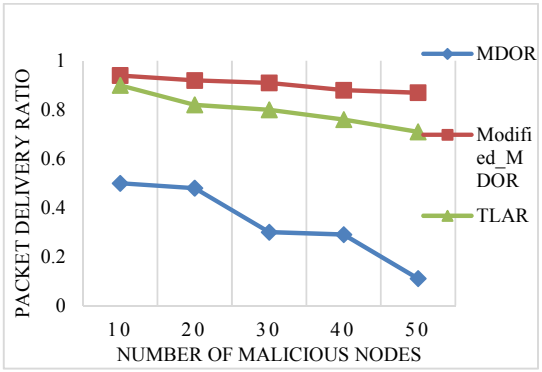


Figure 6.1 Packet Delivery Ratio

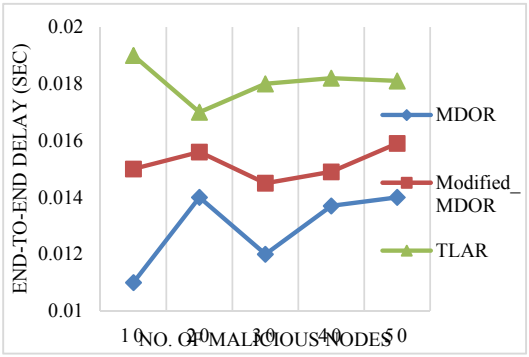


Figure 6.2 End-to-End Delay

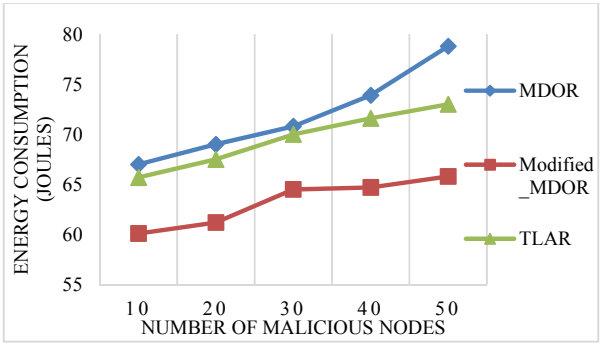


Figure 6.3 Energy Consumption

6.3 TAEROR: OR Protocol for WSN

TAEROR is a trust and reputation aware protocol that is specially designed by taking care of the resource constraints present in WSN. This protocol try to solve the problems in existing trust-aware protocols like high energy consumption, end-to-end delays, low network lifetime and low throughput.

The trust value incorporates the probability of a node being malicious (Pm), forwarding sincerity (F), acknowledgement sincerity (ACK) and energy depletion (E).

$$P_m = (1 - R_U) - R_{delay}$$

$$R_U = N_{dr} / N_s$$

Where, N_{dr} is the number of dropped packets by a node and N_s is the number of packets sent towards the same node.

$$R_{delay} = N_{delay} / N_s$$

Where N_{delay} is the number of packet which are delayed by a node and N_s is the number of packets sent towards the same node.

Forwarding sincerity: Suppose there are two nodes i and j for which we want to calculate the values of these parameters. The forwarding sincerity (F(i, j)) is calculated as follows.

$$F(i,j) = \frac{SF_{(i,j)}}{SF_{(i,j)} + UF_{(i,j)}}(1 - P_m)$$

Where, $SF_{(i,j)}$ is the number of successful packet forwarding from i to j and $UF_{(i,j)}$ is the number of unsuccessful packet forwarding from i to j

Acknowledgement sincerity: The acknowledgement sincerity has been calculated as follows.

$$ACK(i,j) = \frac{SACK(i,j)}{SACK(i,j) + UACK(i,j)}(1 - P_m)$$

Here, $SACK_{(i,j)}$ and $UACK_{(i,j)}$ are the number of successful and unsuccessful acknowledgement forwarding respectively.

Energy Impact: In the trust value calculation, the energy depletion (E_{impact}) value has been introduced which is being calculated as follows.

$$E_{impact}(i,j) = \frac{E_{Fwd}(j) + E_{Rcv}(j) + E_{ack}(i,j)}{E_{total}(j)}(1 - P_m)$$

Where, $E_{Fwd}(j)$ is the energy required by node j to forward a packet further to its neighbors. Similarly, $E_{Rcv}(j)$ is the energy required by node j to receive the packets from node i and $E_{ack}(i,j)$ is the energy consumed in sending acknowledgement from j to i. $E_{total}(j)$ is the total energy of the node j. Following equation will calculate the new trust value (RT(i,j)) for node j with respect to node i.

$$RT(i,j) = \frac{\alpha * F(i,j) + \beta * E(i,j) + \gamma * ACK(i,j)}{\alpha + \beta + \gamma}$$

Where α, β and γ are the importance factors. Means whichever sincerity factor out of three is most importance will be multiplied with highest value. By including previous behavior of the node j, equation below gives the final trust value (FT(i,j)) for node j with respect to node i.

$$FT(i,j) = \sigma * NewRT(i,j) + \lambda * (1 - \sigma) * OldRT(i,j)$$

Where, $0<\sigma<1$ represents the aging factor and $0<\lambda<1$ represents the weight of the *NewRT(i,j)*.

6.3.1 Relay Selection Algorithm

To monitor the packet transmission process, data packet forwarding progress (FP) is calculated using distance between source and destination ($Dist_{s,d}$) and distance between the destination and relay nodes($Dist_{ni,d}$)

$$Dist_{i,j} = \sqrt{(co_x_i - co_x_j)^2 + (co_y_i - co_y_j)^2}$$

Where $0 \le i, j \le k$ and $i \ne j$

$$Progress_{n_i}^{s,d} = Dist_{s,d} - Dist_{n_i,d}$$

Where s=source, d=destination, $0 \le n_i \le k$, k is the total number of nodes

Algorithm: Relay Selection (S=Source, D=Destination)

When node S want to send a packet

Let t_{min} be the minimum acceptable trust factor of a node

x be the number of 1-hop neighbors of S

Let FT[Z] be the node trust factor of node Z

Let Max_NH be the maximum number of neighbors which are allowed in forwarder list (FL)

FL= empty

Sort all 1-hop neighbors of S in descending order according to FT[Z]

For (Z=1; FL < Max_NH and Z <= x; Z=Z+1)

Do

    If (FT[Z] >= t_{min}) then

        Add Z's ID in FL

    EndIf

EndFor

If (FL!=empty)

    Broadcast MSG (S, D, FL, t_{min})

EndIf

6.3.2 Experimental Results and Performance Analysis

For the experimental analysis of proposed protocol TAEROR is simulated on NS2. The simulation scenarios are created and results are recorded. Firstly the security performance has been tested by using a number of mischievous nodes faced through the routing mechanism.

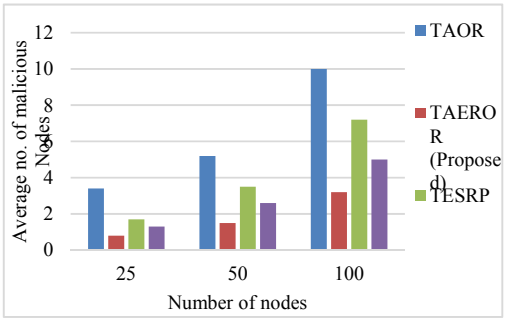


Figure 6.4 Average risk level

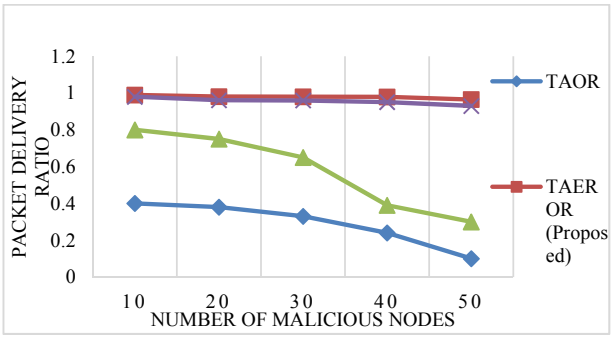


Figure 6.5 Packet Delivery Ratio

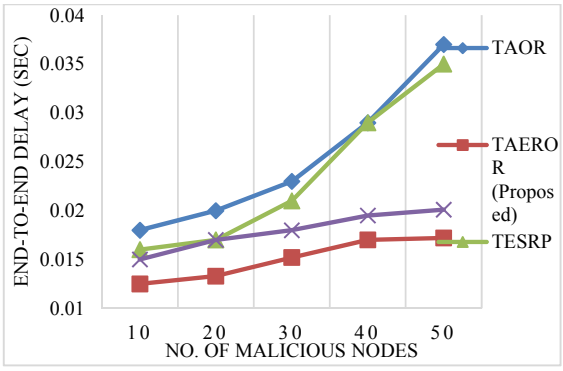


Figure 6.6 End-to-end Delay

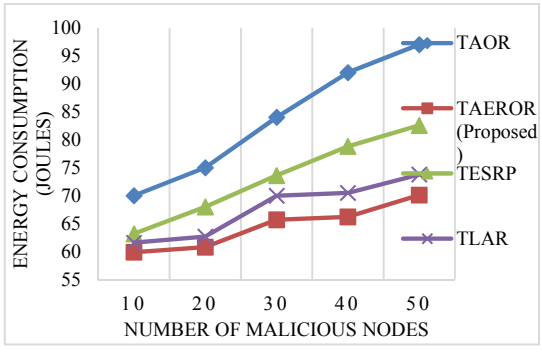


Figure 6.7 Total Energy Consumption

CHAPTER 7

TRUST AND LOAD BALANCING BASED OPPORTUNISTIC ROUTING PROTOCOL

7.1 Introduction

In this chapter, a new trust and energy efficiency aware routing protocol is proposed and named as trust ad packet load balancing OR protocol (TPBOR). TPBOR can directly be employed to WSN and it provides energy efficiency and trust management among all nodes. This protocol also balances the packet load and equalize the number of packets transmitted by each sensor node toward the base station. The protocol will be discussed in the upcoming section.

7.2 Proposed OR Protocol (TPBOR)

The proposed routing protocol specially designed for WSN and hence three major parameters are considered in designing this protocol i.e. trust management, energy efficiency and packet load balancing. TPBOR is an opportunistic protocol and may be used directly with any of WSN applications.

7.2.1 Relay Selection Criteria

In TPBOR the relay selection criteria consist of three phases. The 1st phase the progress of data packet in the network will be measured on the basis of positive distance covered by it toward the base station.

$$Dist_{i,j} = \sqrt{(co_x_i - co_x_j)^2 + (co_y_i - co_y_j)^2} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Where $0 \le i, j \le k$, and $i \ne j$

$$Progress_{n_i}^{s,d} = Dist_{s,d} - Dist_{n_i,d} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(2)$$

Where s=source, d=destination, $0 \le n_i \le k$

The 2nd phase is to the buffer of each node in the forwarder set will be tested. The buffer size of each node is limited.

$$Queue_Test_i = w.\frac{Q_{num}}{Q_{size}} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(3)$$

Where Q_{num} is the number of packets stored currently in the queue, Q_{size} is the total size of the queue of a node and w is the weighting factor. In the 3rd phase, the trust value for each node will be calculated as proposed in chapter 5. Trust value will shortlist the forwarder set according to the behavior of the nodes in the forwarder set.

$$T_i = \frac{\alpha * F_i + \beta * E_{total_i} + \gamma * ACK_i}{\alpha + \beta + \gamma} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(4)$$

Where $0 \leq \alpha, \beta, \gamma \leq 1$ and F_i, E_{totali}, and ACK_i are forwarding sincerity, energy depletion value, and acknowledgment sincerity respectively.

7.2.2 Trust and Packet load Balancing Based OR (TPBOR)

Algorithm: Relay_Selection (S, D, Distance(S, D)) **Input**: Source node S, Destination D, Distance (S, D) **Output**: Successful transmission of a data packet from S to D
1. Create neighbor *NGH* for S 2. Broadcast RTS from S 3. Add the replying node to *NGH* 4. If D belongs to *NGH* 5. Stop algorithm 5. Create *FL* as forwarder list for S 6. For each node in *NGH* 7. Calculate *Queue_Test* using equation 3 8. If *Queue_Test* ($node_i$)>=0.25 then 9. Add $node_i$ to *FL* 10. For each node in *FL* 11. Calculate Trust value (*T*) using equation 4 12. If T ($node_i$) <0.2 13. Discard $node_i$ from FL 14. else 15. Select the node having the largest trust value as next hop forwarder (*FD*) 16. Relay_Selection (FD, D, Distance(FD, D))

7.3 Experimental Results and Performance Analysis

TPBOR has been tested on NS2 by creating simulation scenario. Table 7.1 below depicts the simulation settings in the NS2 environment.

7.3.1 Results

Figure 7.2 below shows the safety performance of all compared protocols i.e. BAOR [15], TLAR [12] and TPBOR. The safety has been measured as the average number of malicious nodes encountered during the routing process. TPBOR has encountered very less number of malicious nodes as compared to other two algorithms.

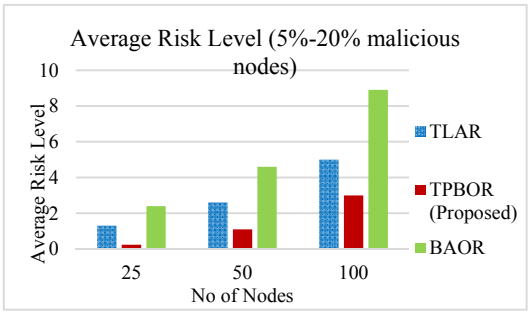


Figure 7.1 Average risk level

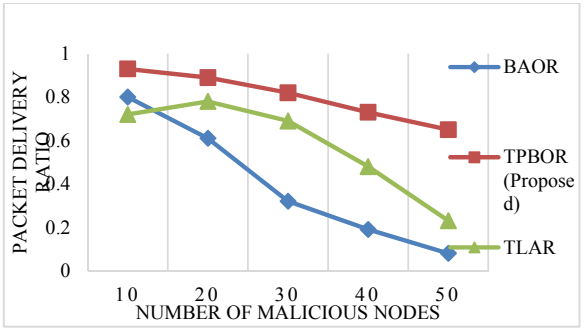


Figure 7.2 Packet Delivery Ratio

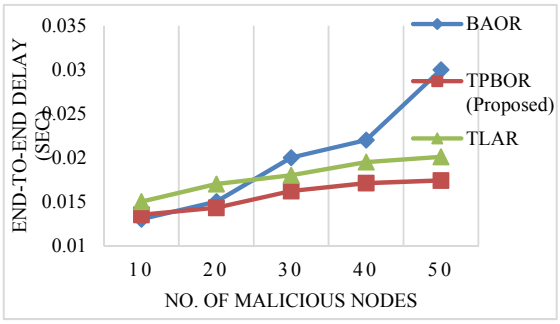


Figure 7.3 End-to-end Delay

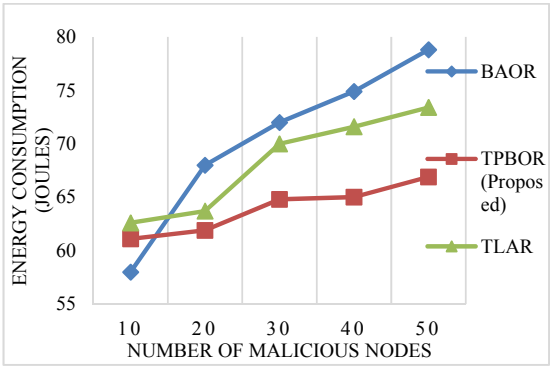


Figure 7.4 Total Energy Consumption

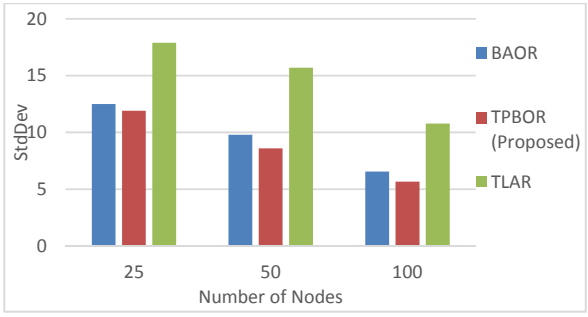


Figure 7.5 Average Number of Packets Transmitted by each Node

Figure 7.6 presents the analysis on the basis of the standard deviation of a number of packets transmitted by each node during the network operation.

$$stdDev = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(n_i - \mu)^2} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (5)$$

CHAPTER 8

CONCLUSION AND FUTURE SCOPE OF WORK

8.1 Introduction

In this thesis, the routing protocols for WSN were studied and categorized. The primary objectives of the thesis were classified into three categories i) reducing energy consumption during network operations to improve the network lifetime, ii) providing security to route selection process by means of trust and reputation and iii) optimizing the packet load, energy efficiency and security of route selection. Other contributions of thesis involved reducing end-to-end delays and path loss and improving the throughput of the network.

8.2 Comparative Analysis

Overall this thesis presented contributions toward the opportunistic routing as well as routing for wireless sensor networks. There were three trust-aware and resource optimization based protocols proposed in Chapter 6 and Chapter 7. These protocols have certain differences among them. TPBOR protocol presented in Chapter 7 presented the optimized results in terms of packet load, energy efficiency and trust management among all the nodes of the network. The comparative analysis of these three protocols can be seen in table 8.1 below.

Table 8.1 Comparative analysis of Modified_MDOR, TAEROR, and TPBOR

Proposed Protocol	Risk Level	Energy Consumption (Joules)	Packet Delivery Ratio	End-to-End Delay (Sec)	Load Balancing (StdDev)
Modified_MDOR	4.20	68.71	0.76	0.015	17.91
TAEROR	3.61	67.84	0.82	0.016	10.98
TPBOR	3.56	70.52	0.87	0.021	6.10

8.3 Future Perspectives

The future directions for WSN may vary from network structure to, application types to application demands. Different applications have different sensitivity factors. Different network designs have different constraints with respect to varying challenges. The trust-aware protocols proposed in Chapter 6 and Chapter 7 can further be extended to include the more important parameters and the security of route selection process will be enhanced. These protocols may be enhanced to use the feedbacks of other neighbor nodes which are also called as indirect trust evaluation parameters. Also, different applications of WSN have different sensitivity factors, different network designs have different constraints with respect to varying challenges. There are different issues at design level of WSN, like node deployment, heterogeneity, localization and synchronization which needs to be explored further. There are various protocols already developed for WSNs need to be compared with respect to WSNs application classes.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer networks*, vol. 38, no. 4, 393-422, 2002.

[2] I. F. Akyildiz, I. H. Kasimoglu, "Wireless sensor and actor networks: research challenges," *Ad hoc networks*, vol. 2, no. 4, pp. 351-367, 2004.

[3] K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks," *Ad hoc networks*, vol. 3, no. 3, pp. 325-349, 2005.

[4] S. Biswas and R. Morris, "ExOR: Opportunistic multi-hop routing for wireless networks," In Proc. ACM SIGCOMM'05, New York, USA, 2005, pp. 133-144.

[5] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 4, no. 3, p. 15, 2008.

[6] M. Michel, S. Duquennoy, B. Quoitin and T. Voigt, "Load-Balanced Data Collection through Opportunistic Routing," In Proc. International Conference on Distributed Computing in Sensor Systems, Fortaleza, 2015, pp. 62-70.

[7] M. Sharma and Y. Singh, "Middle Position Dynamic Energy Opportunistic Routing for Wireless Sensor Networks," In Proc. IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2015, pp. 948-953.

[8] C. C. Hung, K. C. J. Lin, C. C. Hsu, C. F. Chou and C. J. Tu, "On enhancing network-lifetime using opportunistic routing in wireless sensor networks," In Proc. 19th International Conference on Computer Communications and Networks (ICCCN), Zurich, 2010, pp. 1-6.

[9] X. Mao, S. Tang, X. Xu, X. Y. Li, and H. Ma, "Energy-efficient opportunistic routing in wireless sensor networks," *IEEE transactions on parallel and distributed systems*, vol. 22, no. 11, pp. 1934-1942, 2011.

[10] Z. Zhang, S. Wen, W. Yang and F. Zhao, "Energy-efficient Opportunistic Routing Protocol in Wireless Sensor Networks," *Applied Mechanics & Materials*, vol. 610, pp. 797-807, 2014.

[11] A. Tiab, L. Bouallouche-Medjkoune and S. Boulfekhar, "A new QoS aware and energy efficient opportunistic routing protocol for wireless sensor networks," *International Journal of Parallel, Emergent and Distributed Systems*, vol. 33, no. 1, 52-68, 2017.

[12] P. R. Vamsi and K. Kant, "Trust and Location-Aware Routing Protocol for Wireless Sensor Networks," *IETE Journal of Research*, vol. 63, pp. 1-11, 2016.

[13] A. Ahmed, K. A. Bakar, M. I. Channa and A. W. Khan, "A secure routing protocol with trust and energy awareness for wireless sensor network," *Mobile Networks and Applications*, vol. 21, no. 2, pp. 272-285, 2016.

[14] M. Salehi and A. Boukerche, "Trust-aware opportunistic routing protocol for wireless networks," In Proc. 10th ACM symposium on QoS and security for wireless and mobile networks, 2014, pp. 79-86.

[15] W. Cui, Y. Yao and L. Song, "Buffer-aware opportunistic routing for wireless sensor networks," In Proc. 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, 2017, pp. 268-271.

[16] Z. Liu, C. Wei, C. Qin, H. Li, X. Niu and L. Wang, "POR: A Packet-Based Opportunistic Routing Protocol for Wireless Sensor Networks," In Proc. International Conference on Computer Sciences and Applications, Wuhan, 2013, pp. 158-162.

List of Publications

1. **N. Kumar** and Y. Singh, "Routing Protocols in Wireless Sensor Networks," *Handbook of Research on Advanced Wireless Sensor Network Applications, Protocols, and Architectures*, Hershey, PA, USA: IGI Global, pp. 86-128, 2016. DOI: 10.4018/978-1-5225-0486-3.ch004.
2. **N. Kumar** and Y. Singh, "An Energy Efficient Opportunistic Routing Metric for Wireless Sensor Networks," *Indian Journal of Science and Technology*, vol. 9, no. 32, August, p. 7, 2016, DOI:10.17485/ijst/2016/v9i32 /100197.
3. **N. Kumar** and Y. Singh, "An energy efficient and trust management based opportunistic routing metric for wireless sensor networks," In Proc. Fourth IEEE International Conference on Parallel, Distributed and Grid Computing (PDGC-2016), Waknaghat, India, 2016, pp. 611-616, DOI:10.1109/PDGC.2016.7913196.
4. **N. Kumar**, Y. Singh and P. Kr. Singh, "Reputation-based Energy Efficient Opportunistic Routing for Wireless Sensor Network," *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, vol. 9, no. 3-6, pp. 29-33, 2017.
5. **N. Kumar**, Y. Singh and P. Kr. Singh, "An Energy Efficient Trust-Aware Opportunistic Routing Protocol for Wireless Sensor Network," *International Journal of Information System Modeling and Design (IJISMD)*, vol. 8, no. 2, pp. 30-44, 2017 DOI:10.4018/IJISMD.2017040102.
6. **N. Kumar** and Y. Singh, "Trust and packet load balancing based Secure Opportunistic Routing Protocol for WSN," In Proc. 4th IEEE International Conference on Signal Processing, Computing and Control (ISPCC- 2017), Waknaghat, India, 2017, pp. 463-467, DOI:10.1109/ISPCC.2017. 8269723.

Communicated Paper(s)

7. **N. Kumar** and Y. Singh, "Reducing Energy Consumption and Duplication of packets in WSN: Opportunistic Routing Perspective," *Informatica, An International Journal of Computing and Informatics*.
8. **N. Kumar** and Y. Singh, "Energy Efficient and Packet Load Balancing based OR protocol for WSN," *IETE Journal of Research*.